Saint Louis University Law Journal

Volume 50
Number 4 *(Summer 2006)*

Article 21

2006

The Anti-Money Laundering Provisions of the Patriot Act: Should They Be Allowed to Sunset?

Paul Fagyal

THE ANTI-MONEY LAUNDERING PROVISIONS OF THE PATRIOT ACT: SHOULD THEY BE ALLOWED TO SUNSET?

I. INTRODUCTION

What is the importance of tracking and preventing the financing of terrorism? The National Commission on Terrorist Attacks upon the United States, commonly referred to as the 9-11 Commission, addressed this question directly in the report it produced at the end of its investigation into the terrorist attacks on September 11, 2001 ("9-11").[1] Specifically, the 9-11 Commission recommended that "[v]igorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts."[2] The Commission explained that the primary value of tracking terrorist financing was not necessarily the deprivation of funds available to the terrorists, but rather the information that could be obtained through investigations of the terrorists' financial networks.[3] Often, tracking financial networks may prove more effective than traditional operational law enforcement at shutting down terrorist networks preemptively, particularly when there is an ongoing or long-term investigation.[4] However, this recommendation of the 9-11 Commission Report could be considered preaching to the choir, considering that most of the post 9-11 legislation regarding terrorist financing has been designed with this purpose in mind.[5] It has been argued that even with the exhaustive anti-money laundering controls in effect today, the series of transactions that facilitated 9-11 likely would not have been noticed in time to prevent it.[6] Considering the relatively small

1. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9-11 COMMISSION REPORT, 381–82 [hereinafter 9-11 COMMISSION REPORT].

2. *Id.* at 382.

3. *Id.*

4. *Diplomacy in the Age of Terrorism: What is the State Department's Strategy?: Hearing Before Comm. on International Relations H.R.*, 108th Cong. 67 (2004) (statement of Earl Anthony Wayne, Assistant Secretary, Bureau of Economic and Business Affairs, U.S. Department of State).

5. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 302(b), 115 Stat. 272, 297 (2001) (defining the purposes of Title III of the Patriot Act).

6. Eric J. Gouvin, *Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955, 974 (2003). There is some support for this proposition in the 9-11 Commission Report. The Report notes that the terrorists often secured funding through small transactions that were largely unremarkable. 9-11 COMMISSION REPORT,

transactions that were carried out and the total number of similar transactions that occur around the world in a day, attempting to identify well-disguised transactions benefiting terrorism would appear to be similar to looking for a needle in a very large haystack.[7] The primary anti-money laundering legislation enacted after 9-11 was Title III of the Patriot Act, titled the International Money Laundering Abatement and Anti Terrorist Financing Act of 2001.[8] Although Title III has been criticized as ineffective in preventing day to day transactions that finance terrorism, this Comment concludes that the Act must be judged not on its short term success, but rather on its long term potential in conjunction with traditional law enforcement and global measures. Accordingly, anti-money laundering legislation must be examined with respect to facilitating ongoing and extensive investigations rather than as a tool to prevent individual acts of terrorism. Further, the anti-money laundering provisions of the Patriot Act should be evaluated in light of their ability to disrupt the terrorists' overall financing system. This is largely what Title III of the Patriot Act is poised to do.[9] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001 (the "Patriot Act") was made into law on October 26, 2001, shortly over a month after the attacks on September 11, 2001.[10] Despite coming under heavy fire, the Patriot Act remains intact today, and, in conjunction with previously enacted legislation, is the primary tool that law enforcement officials use to combat terrorist financing and other money laundering crimes. The Act is scheduled to sunset in 2005 unless Congress acts and this comment concludes that Title III should be renewed.[11]

No discussion of terrorist financing would be complete without addressing the issue of money laundering. Money laundering is "an indispensable element of organized criminal activities."[12] It is "the process by which one conceals the existence, illegal source, or illegal application of income, and disguises that income to make it appear legitimate."[13] Experts sometimes refer

supra note 1, at 224. The Report also notes that "no financial institution filed a Suspicious Activity Report (SAR) . . . with respect to any transaction of any of 19 hijackers before 9/11." *Id.* at 528 n.116. However, the fact that the Report emphasizes the importance of addressing terrorist financing indicates that the government realized the legislation should not necessarily target only individual acts of terrorism, but rather the comprehensive financing networks.

7. *See The 9-11 Commission and Efforts to Identify and Combat Terrorist Financing Before the S. Comm. on Banking, Housing and Urban Affairs*, 108th Cong. 2–3 (2004) [hereinafter *The 9-11 Commission*] (statement of John E. Lewis, Deputy Assistant Director, Counterterrorism Division, Fed. Bureau of Investigation).

8. USA Patriot Act § 302(b).

9. *See id.* (defining the purposes of Title III of the Patriot Act).

10. *Id.*

11. *Id.* §224.

12. Christopher Boran, *Money Laundering*, 40 AM. CRIM. L. REV. 847, 848 (2003).

13. *Id.* at 847.

to the money laundering process involved in financing terrorism as "reverse money laundering," because the money sought to be laundered is often obtained from legitimate sources and then funneled to illegal purposes.[14] However, the process is substantially similar to traditional money laundering, where the source is illegal but the use legitimate.[15]

Since 9-11, money laundering has received substantially more attention, which is due in large part to leads that may prove that the attacks were partially funded by laundered money.[16] Prior to 9-11, money laundering legislation was primarily backward looking.[17] The authorities were interested in using money laundering legislation to prosecute crimes that had already occurred.[18] Prosecutors could charge criminals with violations of anti-money laundering laws that may be easier to prove than the substantive underlying crime, or they could simply tack on money laundering crimes to other charges in order to extend the defendant's sentence.[19] The harm was already done and, at worst, the criminals could reinvest the money in criminal activities. However, in the context of terrorism, failure to prevent money laundering results in more severe consequences.[20] Terrorists may use the money to plan for an attack, or to obtain the materials and supplies needed to carry out an attack.[21] In the case of terrorism, money laundering is a predicate offense, and it becomes more important to stop the process before it is completed.[22] This makes it important to establish legislation that is forward looking.[23]

Part II of this Comment will explain the process of money laundering, focusing in particular on the three stages of the process, followed by a history of anti-money laundering legislation in the U.S. up to and including the enactment of the Patriot Act. The Comment will focus on the provisions of the

14. *See* Stefan D. Cassella, *International Money Laundering: From Latin America to Asia, Who Pays?*, 22 BERKELEY J. INT'L L. 116, 121 (2004); W. Clifton Holmes, *Strengthening Available Evidence-Gathering Tools in the Fight Against Transnational Money Laundering*, 24 NW. J. INT'L L. & BUS. 199, 199 (2003).

15. Robert E. Sims, *Money Laundering and Corruption: Enforcement After September 11th*, 2002 A.B.A. SEC. INT'L L. & PRAC. (Mar. 21–22, 2002) (page unavailable).

16. Kathleen A. Lacey & Barbara Crutchfield George, *Crackdown on Money Laundering: A Comparative Analysis of the Feasibility and Effectiveness of Domestic and Multilateral Policy Reforms*, 23 NW. J. INT'L L. & BUS. 263, 266 (2003).

17. Cassella, *supra* note 14, at 121.

18. *Id.*

19. *See generally* Teresa E. Adams, *Tacking on Money Laundering Charges to White Collar Crimes: What Did Congress Intend, and What Are the Courts Doing?*, 17 GA. ST. U. L. REV. 531, 532–34 (2000) (discussing the practice of tacking on money laundering charges to other crimes).

20. Cassella, *supra* note 14, at 121.

21. *See id.* (noting that terrorists will use such funds to perpetrate deadly attacks).

22. *See id.* (noting that "the idea is not to hide dirty money to make it clean, but to hide clean money until it can be used to do something evil").

23. *See id.* (explaining that there is no specific law that criminalizes reverse money laundering).

Patriot Act that have a substantial impact on U.S. citizens, as these have been criticized most heavily. It will also include a brief discussion of international anti-money laundering actions to the extent that they impact the domestic provisions of Title III of the Patriot Act. This discussion will necessarily include the criticisms that have been leveled at the existing legislation. Part III will detail the advantages of the paper trail created by the provisions of the Patriot Act, addressing several of the primary criticisms that have been leveled against it.

II. MONEY LAUNDERING AND ANTI-MONEY LAUNDERING LEGISLATION

A. The Crime of Money Laundering

The process of money laundering can be divided into three stages, the first of which is placement.[24] The placement stage consists of placing the cash into the financial system.[25] The second stage is layering.[26] This stage involves conducting a number of transactions to conceal the source of the money when it is derived from criminal activity or the existence of the money when it is intended for the financing of illegal activity.[27] The final stage is integration.[28] This involves entering the funds into commerce either for legitimate or illegitimate means.[29] Some experts have criticized dividing the process of money laundering into three distinct stages as it is sometimes unclear where one stage begins and the other ends.[30] Also, concentrating on an old model might prevent legislators from thinking creatively about how to attack money laundering issues.[31] However, both academics and the law enforcement community continue to refer to the different stages when discussing the issue.[32]

1. Placement

The placement stage involves introducing the money into the financial system in a way that it can then be maneuvered through a series of complex transactions so as to conceal the source of the money. The money launderer faces the most risk at this point because "there exists a direct connection

24. SANDEEP SAVLA, MONEY LAUNDERING AND THE FINANCIAL INTERMEDIARIES 10 (2001).
25. *Id.*
26. *Id.*
27. *Id.* at 10–11.
28. *Id.* at 11.
29. SAVLA, *supra* note 24, at 11.
30. *See id.* at 10–11.
31. *See id.* at 11.
32. *Id.*

between the profits and the crime."[33] Also, introducing large amounts of cash into the financial system is likely to attract attention from law enforcement officials.[34] As a result, most anti-money laundering legislation is aimed at this stage of the process.[35] However, the three-stage model has been criticized for placing too much emphasis on the placement stage.[36] In the case of terrorism, the money in question is often deposited before, rather than after, the criminal act.[37] In this case, the placement stage would not occur.[38] This might occur when a wealthy donor seeks to launder funds that are already in the financial system, or when the funds are collected in the name of a charity and remain legitimate until they are funneled to terrorist activities.[39] In these cases, the placement stage occurs when the money is ostensibly legitimate, and legislation aimed at the placement phase is less effective.

The placement of funds into the financial system has become increasingly difficult to detect due to the large number of ways in which to accomplish it.[40] Depositing the funds into a traditional depositary institution is only one of the ways to accomplish the placement stage.[41] Obviously, this would be the most risky considering the extensive regulation of financial institutions and the comprehensive records retained.[42] As a result, money launderers have become adept at sidestepping the financial system.[43] In order to avoid the deposit of large sums of money that may facilitate detection, they use a process called "smurfing."[44] The process of smurfing involves a number of people making small deposits in a number of different depositary institutions so as to avoid detection.[45] Initially, the "smurfs" made deposits only slightly under the amount that would trigger a report.[46] However, banks began to recognize these

33. PETER LILLEY, DIRTY DEALING: THE UNTOLD TRUTH ABOUT GLOBAL MONEY LAUNDERING, INTERNATIONAL CRIME AND TERRORISM 51–52 (2nd ed. 2003).

34. Sims, *supra* note 15 (page unavailable).

35. LILLEY, *supra* note 33, at 52.

36. SAVLA, *supra* note 24, at 10–11.

37. *Id.*

38. *See id.* at 11.

39. Cassella, *supra* note 14, at 121; *see* Alicia L. Rause, *USA Patriot Act: Anti-Money Laundering and Terrorist Financing Legislation in the U.S. and Europe Since September 11th*, 11 U. MIAMI INT'L. & COMP. L. REV. 173, 184 (2003) (explaining that terrorist groups often obtain their financing from "legal" businesses and charities).

40. Madelyn J. Daley, *Effectiveness of United States and International Efforts to Combat International Money Laundering*, 2000 ST. LOUIS-WARSAW TRANSATLANTIC L.J. 175, 179 (2000).

41. *Id.* at 177–78.

42. *Id.* at 177.

43. *Id.* at 178–79.

44. LILLEY, *supra* note 33, at 52.

45. *Id.*

46. *Id.*

as suspicious and report them accordingly.[47] As a result, the amounts have dipped even further, and hence become more difficult to detect.[48] Although many financial institutions are required to maintain anti-money laundering compliance programs that target these operations, with the help of new technology and professionals such as attorneys and accountants, there is an ever increasing number of ways in which to accomplish the placement stage.[49]

The developing process of "smurfing" demonstrates the difficulty of eradicating money laundering. In the U.S., the Constitution requires that the law must be known to the people before they can be held accountable for violating it.[50] However, knowing the law is knowing how to avoid the law. Money launderers, including those seeking to finance terrorism, can avoid many of the events that would trigger a financial institution's reporting requirements with sufficient planning and preparation. Often they will seek the assistance of attorneys, accountants, or other professionals who are familiar with the law and can instruct them on how to avoid detection.[51] As money launderers break up their deposits into smaller increments, and spread them among increasingly varying financial institutions, these institutions are required to report an ever increasing number of transactions.[52] While this process may result in increased exposure for the "smurfers," it also creates more work for regulatory bodies due to the increased number of reports to analyze.[53] Also, as money laundering networks become more dependent on "smurfs," they create wider barriers between the low level operatives making the deposits and the "kingpins" responsible for the underlying crimes, in order to compensate for the increased risk of the operatives being detected and caught.[54]

Another option is to avoid the financial institutions altogether. Money launderers have come up with a number of ways to conceal the source of the money before it is ever entered into the financial system. These include purchasing expensive property and reselling it, and creating legitimate or semi-legitimate businesses that typically deal primarily in cash in order to obscure the source of the money.[55] Businesses that are susceptible to criminal

47. *See id.*

48. *Id.*

49. Daley, *supra* note 40, at 178–79.

50. U.S. v. Anzalone, 766 F.2d 676, 678 (1st Cir. 1985).

51. *See* discussion *infra* Part II.B.2.

52. *See id.*

53. Peter A. Gallo, *SR-IX: Using the Wrong Tool in the Wrong Place*, THE J. OF TURKISH WKLY. (Feb. 2005), *available at* http://www.turkishweekly.net/news.php?id=3427.

54. *See id.* (noting that reporting requirements have "not been spectacularly successful in bringing down the heads of the trafficking syndicates"). Obviously law enforcement officials are more interested in catching those responsible for the underlying criminal activity, rather than low level operatives whose only act may be depositing the money into the financial system.

55. *See, e.g.*, BOB BLUNDEN, THE MONEY LAUNDERERS 20 (2001).

manipulation include non-profit organizations,[56] and businesses that traditionally deal in large amounts of cash.

2. Layering

The second step in the money laundering process, layering, involves moving the money in a way that makes it untraceable, while still retaining control over the money itself.[57] The layering process can be accomplished in a number of ways, most of them involving a large number of transactions that make it increasingly difficult to trace the money to its original source.[58] In fact, one commentator has argued that the term "layering" is misleading, because it indicates that the true ownership of the money can be revealed simply by peeling back the layers.[59] He has claimed that in reality, the process could more accurately be termed "kaleidoscopic in nature," a multitude of parallel, rather than progressive transactions.[60] The crime of money laundering becomes considerably more difficult to detect at the layering stage.[61] Often at this stage the money has been divided into smaller amounts, and perhaps even mixed in with legitimate funds.[62] Also, due to the developments in technology and globalization, money is becoming easier to move not only between different accounts and financial institutions, but between different nations.[63] However, there are a number of traits that might indicate money laundering activities. Among these are (1) seemingly nonsensical financial transactions, (2) large numbers of sales and purchases of investments subject to commissions, (3) numerous accounts, seemingly unconnected, being consolidated into a smaller number of accounts, and (4) "lack of concern over losses on investments, bank charges or professional advisor charges."[64] Money launderers are generally not concerned with losses or charges, as their primary concern is eliminating the paper trail.

56. Non-profit organizations are often used by terrorist organizations, leading the Financial Action Task Force on Money Laundering to specifically include increased scrutiny for these organizations in their Eight Recommendations on Terrorist Financing. *See* Financial Action Task Force on Money Laundering: Special Recommendations on Terrorist Financing (Oct. 31, 2001), http://www1.oecd.org/fatf/pdf/SRecTF_en/pdf.

57. SAVLA, *supra* note 24, at 13.

58. *Id.*

59. *Id.*

60. *Id.*

61. *See id.*

62. Hence the term sometimes given to the layering stage is "commingling." LILLEY, *supra* note 33, at 53.

63. *Id.* at 4.

64. *Id.* at 53.

One of the primary tools of money launderers during the layering stage is the use of off-shore banks with stringent bank secrecy laws.[65] The banks in these jurisdictions often have very lax reporting requirements, and are susceptible to abuse by criminal activity, whether intentional or not.[66] The U.S. has made progress in the period of time since 9-11 in facilitating information-sharing with many of these countries.[67] However, much of this information-sharing is predicated upon the U.S. providing probable cause of criminal activity unrelated to tax evasion.[68] The reporting has not reached a level where it is automatically provided for analysis, but rather reactively when criminal activity is already suspected.[69] Therefore, once the money has worked its way into the banking systems of these jurisdictions, it will rarely be detected independently of separate criminal investigation.[70] Legislators must focus on agreements with other countries, particularly those considered off-shore banking countries, if they are to have any success in stopping money laundering after the placement stage.[71]

With the use of technology, money laundering can be facilitated by moving money between accounts and through intermediaries in off-shore accounts simply by using a computer service.[72] Due to the overwhelmingly large number of electronic and wire transactions that occur each day, it would be impractical to monitor them all, even with international cooperation.[73]

3. Integration

The final stage of the money laundering process is the integration of the funds back into commerce. At this time the money has been divided up, possibly intermingled with legitimate funds, and moved between a number of banks, accounts, and nations, making it almost impossible to trace.[74] If the

65. Martin A. Sullivan, *U.S. Citizens Hide Hundreds of Billions in Cayman Accounts*, 34 TAX NOTES INT'L 898, 902 (2004).

66. *Id.*

67. *Id.* at 903.

68. *Id.* at 903–04.

69. *Id.*

70. SAVLA, *supra* note 24, at 14.

71. Several international organizations such as the Organisation for Economic Cooperation and Development (OECD), Financial Action Task Force on Money Laundering (FATF), and Financial Stability Forum have been targeting offshore bank secrecy for a number of years through blacklists and sanctions. *See* Bruce Zagaris, *The Merging of the Anti-Money Laundering and Counter-Terrorism Financial Enforcement Regimes After September 11, 2001*, 22 BERKELEY J. INT'L L. 123, 136–37 (2004).

72. JEFFREY ROBINSON, THE LAUNDRYMEN: INSIDE MONEY LAUNDERING, THE WORLD'S THIRD-LARGEST BUSINESS 30–31 (1996).

73. *Id.* at 31. As of 1996, "more than five hundred thousand wire transfers, representing in excess of $1 trillion, electronically circle[d] the globe daily." *Id.*

74. Lacey & George, *supra* note 16, at 295.

money has been laundered successfully, there will be little or no way to determine the original source. This is desirable to terrorists whether the money was originally legitimate or not. If the original source of the funds cannot be determined, then that source can continue to provide funds to other terrorists. It is at this time that the money can be used with relative impunity to purchase the goods or services necessary to implement an attack.

B. Anti-Money Laundering Legislation

Prior to 9-11, little attention was given to anti-money laundering legislation. Money launderers were rarely prosecuted successfully, for a variety of reasons.[75] Also, there was a trend away from requiring reporting from financial institutions due to privacy concerns.[76] Since 9-11, these concerns have been overlooked in part because of the increased scrutiny of terrorism.[77] While civil libertarians leveled significant criticism at much of the legislation in response to the increasingly invasive reporting requirements, others view the legislation as long overdue.[78] Prior to 9-11, the primary tool for combating money laundering 9-11 was the Bank Secrecy Act of 1970 (BSA).[79] After 9-11, the Patriot Act largely amended the BSA in an effort to combat terrorism more effectively by closing loopholes in the BSA and by addressing the international nature of money laundering.[80] The BSA as amended by the USA Patriot Act provides the primary tools used to combat money laundering in the United States.

1. The Bank Secrecy Act

The BSA served as a landmark in the history of money laundering legislation. It was Congress's first foray into the arena of money laundering legislation.[81] The BSA referred to Titles I and II of the Bank Records and

75. Lisa A. Barbot, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L. & COMP. L. 161, 193–98 (1995). These factors may include, among others: (1) the complexity of money laundering; (2) lax anti-money laundering legislation in various parts of the world; (3) tax havens; (4) various bank secrecy laws; (5) corporate secrecy; and (6) attorney–client privilege issues. *Id.* at 194–98.

76. Denise Couture, *Muted Response to U.S. Law*, INT'L HERALD TRIB., Oct. 31, 2001, at 21; Megan Roberts, *Big Brother Isn't Just Watching You, He's Also Wasting Your Tax Payer Dollars: An Analysis of the Anti-Money Laundering Provisions of the USA Patriot Act*, 56 RUTGERS L. REV. 573, 582 (2004).

77. *See* Couture, *supra* note 76, at 21.

78. *Id.* Much of the criticism revolves around the same issues that were dispensed within *California Bankers Assn. v. Schultz*, 416 U.S. 21 (1974).

79. Pub. L. No. 91-508, 84 Stat. 1114; *see* Matthew S. Morgan, *Money Laundering: The American Law and Its Global Influence*, 3 NAFTA: L. & BUS. REV. AM. 24, 26 (1997).

80. *See generally* Zagaris, *supra* note 71, at 133–36.

81. Morgan, *supra* note 79, at 26.

Foreign Transactions Act that became law in 1970.[82] The stated purpose of the BSA was "to require the maintenance of appropriate types of records by insured banks in the United States where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[83] In effect, the BSA sought to create a paper trail with regard to large transactions to be used by government agencies to detect and pursue criminal activity.[84] The BSA did not criminalize the act of money laundering, but rather sought to use the records to prosecute the underlying criminal activity inherent in money laundering. The underlying criminal activities of money laundering range from simple tax evasion to drug trafficking and terrorism.

The BSA has been continuously amended since its enactment, and has been described as a "chess game pitting those seeking to launder illicit monies against those seeking to stop them."[85] This describes the unique qualities of anti-money laundering legislation. Often those who seek to launder money have specialized knowledge of the financial industry, or have retained the services of professionals with such knowledge.[86]

The BSA does not actually specify the type of reports that financial institutions must file, but rather serves as an enabling statute that authorizes the Secretary of the Treasury to promulgate regulations to that end.[87] The most significant contribution to the current anti-money laundering regulatory scheme is a regulation issued by the Secretary of the Treasury that requires financial institutions, as defined by the BSA, to file Currency Transaction Reports (CTRs). The regulation provides that "[w]hen a domestic financial institution is involved in a transaction for the payment, receipt, or transfer of United States coins or currency" over the amount of $10,000, the institution must file a CTR.[88]

The constitutionality of the BSA was challenged shortly after its enactment, and in 1974 the issue came before the Supreme Court in *California Bankers Ass'n v. Shultz*.[89] A group of banks, financial institutions, and their customers sought to enjoin the enforcement of the regulations promulgated by the Secretary of Treasury, claiming, *inter alia*, that the reporting requirements

82. 31 U.S.C. § 5311 (2000).

83. Bank Secrecy Act of 1970 § 101.

84. Zagaris, *supra* note 71, at 125–26.

85. Morgan, *supra* note 79, at 27.

86. Lacey & George, *supra* note 16, at 281–82. Part of the reason that money laundering itself was criminalized in the Money Laundering Control Act of 1986 was to curb the involvement of professionals such as accountants and attorneys in money laundering activities. *Id.* While the professionals may not have been involved in the underlying crimes, and indeed may not have even had knowledge of the underlying crimes, they could still be prosecuted for money laundering offenses. *Id.*

87. *See* Morgan, *supra* note 79, at 28.

88. 31 U.S.C. § 5313(a) (2000); 31 C.F.R. § 103.22(b) (2005).

89. 416 U.S. 21 (1974).

amounted to an unreasonable search and seizure in violation of the Fourth Amendment.[90] The banks were concerned with the costs of implementing the regulations and claimed that the reporting requirements were sufficiently demanding as to constitute a violation of due process.[91] Justice Rehnquist dismissed this due process argument decisively, stating that the issue "[did] not warrant extended treatment."[92] The Court further explained that the BSA was passed only after extensive congressional findings that provided evidence that most of the required records were maintained by banks in the regular course of business.[93] Therefore, it would have been difficult to establish a significant burden on the banks.

The customers, represented by the ACLU, were concerned about the invasion of privacy that resulted from banks disclosing information about their currency transactions.[94] Justice Douglas expressed sympathy for this point of view in his dissenting opinion, explaining that "[i]n a sense a person is defined by the checks he writes."[95] Justice Douglas went on to write that "[b]y examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on *ad infinitum*."[96] Further, Justice Douglas theorized that recording all of our phone conversations would most likely aid criminal investigations, though clearly in violation of the Fourth Amendment.[97] It should be noted in response to Justice Douglas's criticism, however, that most of the records the BSA required to be maintained were generally kept prior to its enactment, distinguishing it from a situation where a person's phone calls were recorded, with no apparent independent purpose.[98] The Court recognized that the purpose of the BSA was merely to insure that all banks met a minimum standard.[99] Moreover, the vast majority of customer transactions would not be reported. Only those that met the reporting requirements, those in excess of $10,000, would be reported automatically.[100] The majority

90. *Id*. at 41.
91. *Id.* at 42–43.
92. *Id.* at 50.
93. *Id.* at 52–53.
94. *California Bankers Ass'n*, 416 U.S. at 43.
95. *Id*. at 85.
96. *Id*.
97. *Id.*
98. U.S. v. Miller, 425 U.S. 435, 442–43 (1976).
99. *Id.*
100. Robert S. Pasley, *Privacy Rights v. Anti-Money Laundering Enforcement*, 6 N.C. BANKING INST. 147, 195 (2002).

> Further, the BSA does not require the banks to "spy" on their customers, but instead to simply retain copies of documents that the banks already possess, to which banks are a party, and that were found to "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings" and to report "abnormally large transactions in

dismissed the claims and upheld the BSA and the regulations promulgated by the Secretary of Treasury, finding that the reporting requirements did not amount to a taking and that there was not a violation of due process as the state had a legitimate interest in the information.[101] The Court focused specifically on the damage that money laundering did to the tax system.[102] Although the Court mentioned the facilitation of criminal activity inherent in money laundering, this was not the primary focus.[103] The Court dismissed the claims based on the filed CTR, holding that customers who did not engage in the type of $10,000 domestic currency transaction requiring reporting lacked standing to challenge the domestic reporting regulations.[104]

Shortly thereafter, the issue again came before the Supreme Court in *U.S. v. Miller*.[105] This time, the Court addressed the customer's complaint and held that customers of banks had no expectation of privacy with regard to information that they had voluntarily disclosed to a third party.[106] The Court went on to explain that when customers disclosed transactional information to the bank, they should expect that the bank would convey the information to the government, regardless of whether the customer expects that the third party will keep the information privileged and use it for a specified purpose.[107] The Court seemed to take the stance that the bank was not acting as a government agent even though the documents in question were maintained pursuant to the BSA. Rather, the Court viewed the records as those that should be kept in the ordinary course of business, for which the BSA set minimum standards.

The decisions in *California Bankers Assn.* and *Miller* were significant because they provided constitutional validity to the regulatory scheme established by the BSA. Thirty years after these cases were decided, they are still relevant because, although the BSA has been amended a number of times, the basic regulatory scheme remains the same. These two cases set the stage for an expansive regulatory scheme based on financial institutions reporting the activity of their customers.

Although the Supreme Court upheld the constitutionality of the BSA, there continue to be critics of the reporting requirements. These critics have

currency." These reportable cash transactions in excess of $10,000 are, in fact, unusual for most individuals and certainly do not constitute "all bank records of every citizen." Nor do these large cash transactions indicate in any way a customer's "religion, ideology, opinions, and interests."

Id. at 197.

101. *California Bankers Ass'n.*, 416 U.S. at 50–52.

102. *Id.* at 27–28.

103. *Id.* at 26–30.

104. *Id.* at 68.

105. 425 U.S. 435 (1976).

106. *Id*. at 443.

107. *Id*.

expressed concern over the fact that the financial institutions are essentially forced to spy on their own customers.[108] One commentator analogized the BSA reporting requirements to "effectively deputizing bank tellers to act as law-enforcement agents against their own customers."[109] Privacy issues were raised by legislators prior to the bill's enactment, and continued to be of concern, until the 9-11 attacks largely quieted the movement.[110]

During the period after the BSA was first enacted, many financial institutions failed to fully comply with the regulations.[111] It was not until February 1985, when the U.S. Treasury fined the Bank of Boston $500,000 for a failure to report over 1,100 transactions totaling over $1.6 billion that the banking industry began to take the regulations seriously.[112] In part, this led to the Money Laundering Control Act of 1986 (MLCA).[113] However, thirty-four years after its enactment, although revised a number of times, the BSA continues to provide one of the most commonly used tools in fighting money laundering, and financial institutions may face stiff penalties for the failure to adhere to it.[114] The approach to money laundering established by the BSA is largely still intact, and continues to inform efforts to address the issue.

2. The Money Laundering Control Act of 1986

In 1986, Congress determined that the BSA as enacted had not been effective in controlling money laundering.[115] As a result, Congress enacted the MLCA as a part of the Anti-Drug Abuse Act of 1986.[116] The MLCA went a step further than the BSA, and actually criminalized the act of money laundering.[117] The MLCA also protected financial institutions from civil liability for providing information to the government, referred to as "safe harbor" provisions.[118] It also addressed the inflexible reporting requirements

108. Lacey & George, *supra* note 16, at 304–05.

109. David S. Cloud & Jacob M. Schlesinger, *Treasury Seeks to Ease Costliness of Antilaundering Rules on Banks*, WALL ST. J., June 7, 2001, at A4.

110. Lacey & George, *supra* note 16, at 304.

111. *See* Morgan, *supra* note 79, at 28–29.

112. *Id.*

113. Pub. L. No. 99-750, 100 Stat. 3207; *see* Morgan, *supra* note 79, at 29.

114. *See, e.g.*, Robert G. Bagnall, *Anti-Money Laundering*, SJ095 ALI-ABA 222, 236–37 (2004). In July 2001, U.S. Trust Corporation consented to a $10 million civil penalty for failing to "maintain proper controls and procedures relating to BSA compliance." *Id.* at 236. A few months later, in November 2001, the State Bank of India consented to a $7.5 million penalty for similar conduct. *Id.*

115. Morgan, *supra* note 79, at 29.

116. Pub. L. No. 99-570, 100 Stat. 3207; *see* Morgan, *supra* note 79, at 29; Zagaris, *supra* note 71, at 126.

117. Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 (1986) (codified as amended at 18 U.S.C. § 1956, 1957) [hereinafter MLCA].

118. Lacey & George, *supra* note 16, at 293–96.

created by the BSA.[119] Under the BSA, only transactions that exceeded the amount prescribed by the Secretary of Treasury ($10,000) would be reported.[120] Money launderers became adept at smurfing (breaking up the transactions to smaller amounts) to avoid drawing attention.[121] Courts were split regarding whether structuring the transactions violated the statute.[122] As a result, the MLCA criminalized the act of structuring transactions in order to "cause or attempt to cause a domestic financial institution to fail to file a [required report]."[123] This was largely in response to the confusion by both the courts and the financial institutions regarding whether structuring violated the regulations as promulgated by the Secretary of the Treasury.[124] A number of banks were already filing CTRs when deposits were structured in a way to avoid reporting requirements.[125]

Financial institutions may face stiff penalties for failing to observe the aggregation reporting requirements. The Financial Crimes Enforcement Network (FinCen), the agency responsible for enforcing the BSA and subsequent amendments, including the Patriot Act, recently issued an opinion regarding aggregating transactions in a case involving Western Union.[126]

119. Jimmy Gurule, *The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?*, 32 AM. CRIM. L. REV. 823, 825 (1995).

120. *Id.*

121. *Id.*

122. The regulation promulgated by the Secretary of the Treasury in accordance with the BSA stated:

> Each financial institution shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution, which involves a transaction in currency of more than $10,000. Such reports shall be made on forms prescribed by the Secretary and all information called for in the forms shall be furnished.

31 C.F.R. § 103.22(a) (1980). The courts took a variety of positions regarding whether "smurfing" or structuring deposits to avoid the filing requirements violated the statute. The First Circuit held that the regulations as written violated the Fifth Amendment due process clause. U.S. v. Anzalone, 766 F.2d 676, 682 (1st Cir. 1985). The Seventh Circuit held that the banks had no duty to report transactions under the $10,000 ceiling, and thus structuring deposits did not constitute a crime. U.S. v. Gimbel, 830 F.2d 621, 624 (7th Cir. 1987). At the other end of the spectrum, the Second Circuit appeared to adopt a policy it referred to as structural liability, and held that structuring transactions so as to avoid reporting requirements was a crime. U.S. v. Heyman, 794 F.2d 788, 792 (2d Cir. 1986). The issue became moot when the MLCA was passed, as it specifically criminalized the structuring of transactions. Pub. L. No. 99-570, § 1354, 100 Stat. 3207 (1986) (codified as amended at 31 U.S.C. § 5324 (2002)).

123. Money Laundering Control Act of 1986 § 1354.

124. *See supra* text accompanying note 122.

125. *Id.*

126. *In re* Western Union Financial Services, Inc., No. 2003-02, Treas. Dep't Fin. Crimes Enforcement Network (Mar. 6, 2003), *available at* http://www.fincen.gov/western_union_assessment.pdf).

Western Union consented to a civil penalty of $3 million.[127] In the opinion, FinCen reiterated previous findings that transactions made by the same person, or on behalf of the same person and known to the financial institution, must be aggregated with regard to the CTR reporting requirements, even if they are made among different agents.[128]

The legislative history of the MLCA does not indicate any significant interest in terrorism.[129] Rather, Congress seemed more concerned with professionals in legitimate businesses turning a blind eye to clients that were involved in money laundering schemes.[130] This was criminalized in the MLCA, which makes it illegal to knowingly engage in a transaction for an amount of more than $10,000 where the money is derived from unlawful activity.[131] The government does not need to prove the defendant had knowledge that the money was derived from unlawful activity, only that the defendant knowingly engaged in the transaction.[132] The purpose was to eliminate the defense of willful blindness by professionals with specialized knowledge of money laundering laws.[133] In effect, the Act was used mostly to prosecute those involved in drug sales.[134] Some scholars claimed that the MLCA did not define a new type of illegal conduct, but rather allowed new ways to prosecute underlying offenses that may have been more difficult to prove.[135] As a result, the MLCA added little to the detection and prosecution of those who finance terrorism.[136] The MLCA's primary contribution was the criminalization of money laundering.[137]

3. The Annunzio–Wylie Anti-Money Laundering Act of 1992

The Annunzio–Wylie Anti-Money Laundering Act of 1992[138] was passed in response to inflexibility in the existing anti-money laundering scheme.[139] It

127. *Id.* at 5.

128. *Id.* at 2.

129. *See generally* Lacey & George, *supra* note 16, at 291.

130. Gurule, *supra* note 119, at 825.

131. Money Laundering Control Act of 1986, Pub. L. No. 99-570, § 1352, 100 Stat. 3207 (codified as amended at 18 U.S.C. § 1957 (2000)).

132. *See* Lacey & George, *supra* note 16, at 292 (explaining that "[t]he government must prove: 1) that illicit funds were derived from one of the [specified unlawful activities] in the statute; and 2) that the defendant engaged in the [specified unlawful activity], then laundered the illicit proceeds").

133. Gurule, *supra* note 119, at 825.

134. *See id.* at 853–54.

135. *See id*.

136. *See id*. at 853 (arguing that Congressional intent was limited to attacking the activities of "post-crime hiding and reinvesting of illicit profits to continue proscribed criminal activity").

137. *See id.*

138. Pub. L. 102-550, 106 Stat. 4044 (1992) (codified as amended in scattered sections of Titles 12, 18, and 31 of the U.S. Code).

was becoming apparent to legislators that money launderers were becoming increasingly sophisticated, and quickly adapting to anti-money laundering legislation.[140] CTRs are inflexible, and law enforcement officials felt that a significant amount of illegal activity was still going unnoticed due to "smurfing."[141] As a response, the Annunzio–Wylie Anti-Money Laundering Act created the Suspicious Activity Report (SAR),[142] and in effect shifted to the banking community the responsibility of determining which transactions should be reported.[143] The Act specifically prohibited notifying the subject of the SAR that he had been reported.[144] The constitutional validity of the SAR has not been seriously challenged. However, courts have had the opportunity to consider the prohibition on notification of the subject of the report. The courts have recognized that the state has a legitimate interest in keeping the SAR confidential so as not to "compromise an ongoing law enforcement investigation, provide information to a criminal wishing to evade detection, or reveal the methods by which banks are able to detect suspicious activity."[145] According to the regulations promulgated by the Secretary of the Treasury, financial institutions were required to file a SAR with the proper regulatory authority for "any suspicious transaction relevant to a possible violation of law or regulation."[146] The regulations also lowered the threshold amount from $10,000, as required by a CTR, to $5,000.[147] The Act provided for strict liability for the failure to file a report, while at the same time providing immunity to the financial institutions for filing an unnecessary report in good

139. Mariano-Florentino Cuellar, *The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93 J. CRIM. L. & CRIMINOLOGY 311, 362–63 (2003); *see also* Patricia Shaughnessy, *The New EU Money-Laundering Directive: Lawyers As Gate-Keepers and Whistle Blowers*, 34 LAW & POL'Y INT'L BUS. 25, 25 (2002) ("As developments in technology and in the financial sector allowed for increasingly complex transnational transactions, money-launderers became more sophisticated, employed new channels, and became linked not only with drug traffickers, but also with other criminal groups, including terrorists.").

140. *See* Cuellar, *supra* note 139, at 362–63.

141. *See* Gouvin, *supra* note 6, at 967.

142. Annunzio–Wylie Money Laundering Act of 1992 § 1517; *see also* Gouvin, *supra* note 6, at 967.

143. Morgan, *supra* note 79, at 41–42.

144. Annunzio–Wylie Money Laundering Act of 1992 § 1517(g)(2).

145. Whitney Nat'l Bank v. Karam, 306 F. Supp. 2d 678, 680 (S.D. Tex. 2004); *see also* Cotton v. PrivateBank & Trust Co., 235 F. Supp. 2d 809, 815 (N.D. Ill. 2002) ("[T]he disclosure of [a] SAR may harm the privacy interests of innocent people whose names may be contained therein.").

146. 31 C.F.R. § 103.20(a)(1) (2005).

147. 31 C.F.R. § 103.20(a)(3).

faith.[148] The result was the "generation of large numbers of extraneous reports," reporting mostly innocent activity.[149]

The Annunzio–Wylie Anti-Money Laundering Act also required that each financial institution implement an Anti-Money Laundering Program.[150] The Secretary of the Treasury was required to implement regulations that would require at a minimum: "(A) the development of internal policies, procedures, and controls, (B) the designation of a compliance officer, (C) an ongoing employee training program, and (D) an independent audit function to test programs."[151]

Both the SAR and the anti-money laundering program provisions are still intact today, and have been significantly expanded by the Patriot Act.

4. The Patriot Act

Shortly after the attacks on 9-11, Congress passed the Patriot Act in response to the new focus on terrorism.[152] Significant criticism has been aimed at the Patriot Act since its enactment regarding the method in which it was

148. Gouvin, *supra* note 6, at 967–68. The immunity only extends to reports made to law enforcement agencies. Nevin v. Citibank, N.A., 107 F. Supp. 2d 333, 342 (S.D.N.Y. 2000) (holding that a financial institution was not immune from suit when the SAR was provided to another private party). However, the financial institutions are immune from liability for a variety of disclosures, including "(i.) A disclosure of any possible law or regulation, (ii.) A disclosure pursuant to § 5318(g) itself, or (iii.) A disclosure pursuant to *any other authority*." Coronado v. BankAtlantic Bancorp, Inc., 222 F.3d 1315, 1319 (11th Cir. 2000) (emphasis added) (holding that a grand jury subpoena qualifies as "other authority," that safe harbor is not limited to CTR, and that any provision grants the financial institution complete immunity). *But see* Lopez v. First Union Nat'l Bank of Fla., 129 F.3d 1186, 1193 (11th Cir. 1997) (holding that "verbal instructions" did not qualify as "other authority" under safe harbor provisions).

149. Gouvin, *supra* note 6, at 967. Although innocent conduct is routinely reported, the courts have protected the privacy interest of the subject of the SAR. While the information is provided to the government, the courts have not allowed the documents to be provided to third parties. *See Cotton*, 235 F. Supp. 2d at 814 (holding that SAR was not discoverable, but documents of underlying transaction were); *see also Karam*, 306 F. Supp. 2d at 682–83.

> [Financial institutions] are protected from the production of communications they made to governmental agencies or officials reporting possible or suspected violations of laws or regulations by the defendants, or pertaining to such reports. Such communications may consist of a SAR itself; communications pertaining to a SAR or its contents; communications preceding the filing of a SAR and preparatory or preliminary to it; communications that follow the filing of a SAR and are explanations or follow-up discussions; or oral communications or suspected or possible violations that did not culminate in the filing of a SAR.

Id.

150. Annunzio–Wylie Money Laundering Act of 1992, Pub. L. 102-550, § 1517(h), 106 Stat. 4044 (1992) (codified as amended in 31 U.S.C. § 5314).

151. *Id.*

152. Lacey & George, *supra* note 16, at 291.

passed. The bill saw almost no opposition in either the House or the Senate.[153] After the Patriot Act became law, it was discovered that many legislators either did not attempt to, or did not have time to, study the provisions of the Act before they had to vote.[154] While this is certainly a disturbing commentary on the state of Congress, careful study might not have had as large of an effect on the final form of Title III as it would have had on other provisions of the Patriot Act.[155] Much of the legislation included in Title III has been debated in the public arena for a number of years, even dating back to the 1970s when money laundering legislation first came into play with the BSA.[156] Although some have criticized the legislation based on the fact that it was defeated a number of times, this may also indicate that the legislation was not quite as rushed as it seemed. Rather, one could determine that 9-11 provided the motivation, or increased state interest, that was necessary to justify the increased imposition on financial institutions.[157] The amendments to the BSA in the Patriot Act expanded the reach of the BSA and subjected a number of new financial institutions, including informal money transfer services, to the reporting requirements previously enacted.[158] These institutions were also required to implement anti-money laundering provisions.[159] The Patriot Act also requires banks and other financial institutions to implement customer identification programs, commonly referred to as "know your customer" (KYC) provisions.[160] As a preliminary matter, it should be noted that the Patriot Act did not significantly alter the nature of the regulatory scheme, but rather expanded the existing scheme.

a. Industries Subjected to BSA Requirements

The industries that are subject to the anti-money laundering provisions after the enactment of the Patriot Act are "mutual funds; operators of credit card systems; money services businesses, such as money transfer companies and check cashers; securities brokers and dealers registered with the Securities

153. Gouvin, *supra* note 6, at 960–61.

154. *Id.*

155. *But see* Gilbert NMO Morris, *Issues in Title III Compliance Under the USA Patriot Act*, 28 TAX NOTES INT'L 385, 387 (2002).

156. *See* Gouvin, *supra* note 6, at 963; Lacey & George, *supra* note 16, at 300–01 (summarizing proposed legislation that was not enacted from 1998–2001).

157. See Lacey & George, *supra* note 16, at 290–91; *see also* Michael T. McCarthy, *USA Patriot Act*, 39 HARV. J. ON LEGIS. 435, 451 (2002) (suggesting that the sweeping legislation in the Patriot Act might not have been solely a rushed power grab, but rather that "lawmakers may have reached a measured conclusion that the attacks had indeed changed assumptions about the nature of the threat to domestic security, and that prior political conceptions about executive authority were no longer apt").

158. Gouvin, *supra* note 6, at 970.

159. *Id.* at 971.

160. *Id.* at 970.

and Exchange Commission; and futures commission merchants and accompanying introducing brokers registered with the Commodity Futures Trading Commission."[161] One of the requirements was that they file SARs. According to 12 C.F.R. § 21.11, banks and other financial institutions must file a SAR with FinCEN when

> the bank knows, suspects, or has reason to suspect that: (i) [t]he transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities . . . as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law; (ii) [t]he transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or (iii) [t]he transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.[162]

The Patriot Act also shored up the "safe harbor" provision, so that financial institutions are largely immune for filing SARs unnecessarily.[163] Congress entrusted the enforcement of the Patriot Act and previous BSA provisions to FinCEN.[164]

SARs are generally completed by those who come into direct contact with depositors of money. A potential problem of SAR reporting is that there is little motivation to report this activity. Unlike other crimes where there is an identifiable victim, the ultimate harm of money laundering is not quite as apparent.[165] Suspicious Activity Reports often require the initiative of relatively low level operatives within an organization, who may be deterred by the extensive reporting requirements. The Treasury Department has outlined

161. Morris, *supra* note 155, at 390.

162. 12 CFR § 21.11(c)(4) (2005).

163. The Patriot Act provided:

> Notwithstanding any other provision of this title, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a governmental agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

Patriot Act, Pub. L. No. 107-56, § 626(e), 115 Stat. 272, 328 (2001) (codified as amended at 15 U.S.C. § 1681). Section 302(b)(9) of the Patriot Act stated that one of the purposes was "to clarify the terms of the safe harbor from civil liability for filing suspicious activity reports." § 302(b)(9).

164. Patriot Act § 361.

165. *See* Daley, *supra* note 40, at 179 ("Money laundering is a paperless crime, without physical violence directed at individuals.").

specific circumstances in which a CTR is required.[166] Financial institutions therefore generally have little difficulty determining when a CTR should be filed. However, the situations in which an SAR is required are less specific. While many large depositary institutions have created a position for a compliance officer, and have attempted to instruct the lower-level operatives of what these situations might be, there is still a high degree of discretion at the lower levels. Money laundering can most easily be detected by employees who have a personal exchange with the money launderer.[167] In the case of the largest money transfer company, Western Union, the employees responsible for completing the SARs might not even be employees of Western Union.[168] Many Western Union locations are operated by independent contractors who provide the money transfer service via Western Union, but are employed by the facility from which the service is offered.[169] The limited relationship between Western Union and the independent contractor may make it even more difficult for Western Union to enforce and monitor compliance with the reporting requirements.[170]

Significantly, section 359 of the Patriot Act extends financial reporting requirements to informal value transfer systems (IVTS).[171] The Patriot Act also establishes criminal penalties for unlicensed money transfer services.[172] This requirement appears to be aimed at *hawalas*, which are a type of IVTS

166. *See* discussion *supra* Part II.B.1.

167. Lacey & George, *supra* note 16, at 281.

168. Heather Timmons, *Terrorist Money by Wire*, BUS. WK., Nov. 5, 2001, at 94.

169. *Id.* The investigation into 9-11 has provided evidence that many of the terrorists involved in the attack transferred or received money through Western Union terminals in places such as a Mail Boxes, Etc. and Giant Supermarket in Laurel, Maryland. Heather Timmons, *Western Union: Where the Money Is—In Small Bills*, BUS. WK., Nov. 26, 2001, at 40. There were also transfers in and out of Logan Airport and the Boston bus station. *Id.*

170. Western Union recently settled an action brought by New York's banking regulators for $8 million without admitting wrongdoing. Gouvin, *supra* note 6, at 965. The regulators alleged that Western Union had violated state and federal currency transaction reports. *Id.*

171. *See* Patriot Act, Pub. L. No. 107-56, § 359, 115 Stat. 272 (2001) (codified as amended at 31 U.S.C. §§ 5312, 5318, 5330).

172. *Id.* § 373. The section defines unlicensed money transmitting business as one that

> (A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;
>
> (B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or
>
> (C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used . . . to promote or support unlawful activity.

Id.

that ties much of the Islamic world together financially.[173] The purpose of these systems is to transfer value between people, often in different countries, without actually moving the money.[174] The potential value to terrorists is that the process leaves a sparse money trail, if a trail exists at all. The process is relatively simple. An individual will go to a *hawaladar* in one country and request that money be transferred to an individual in another country.[175] The *hawaladar* will give the individual wishing to transfer money a code, which he will then communicate to the recipient.[176] The *hawaladar* will contact another *hawaladar* in the target country and instruct him to pay an amount of money to the recipient upon presentation of the code.[177] The two *hawaladars* will then settle for the balance in some other type of transaction.[178] This can include a more formal transaction, or invoice manipulation.[179] These systems have been in existence for an extended period of time, and the vast majority of IVTS activity appears to be legitimate in purpose.[180] "In countries lacking a stable financial sector or containing substantial areas not served by formal financial institutions, IVTS may be the only method for conducting financial transactions."[181] These types of IVTS can also be used when immigrants are sending small amounts of money home to their families and formal value transfer systems are too expensive.[182] Reports have been mixed with regard to the success of regulating these industries. The same factors which make this type of transfer inexpensive also contribute to its potential for abuse. Although it is currently impossible to estimate with any accuracy the amount of money that changes hands through this system, it has been estimated to be in the tens of billions of dollars annually.[183] Even if this industry was not years behind its

173. Gouvin, *supra* note 6, at 977–78. Hawalas are not the only type of IVTS. ROBINSON, *supra* note 72, at 14. These systems have been around for a significant period of time, and are generally the result of political turmoil or a distrust of banks. *Id.* Although other types of IVTS exist in the U.S., considering the timing and purpose of the Patriot Act, it most likely sought to regulate *hawalas*, considering the strong ties to Islam, and evidence that the system has been used for terrorist purposes. *See* Gouvin, *supra* note 6, at 978–79.

174. *See* Rachana Pathak, *The Obstacles to Regulating the Hawala: A Cultural Norm or a Terrorist Hotbed?*, 27 FORDHAM INT'L L.J. 2007, 2011–15 (2004).

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.*

179. Pathak, *supra* note 174, at 2011–15.

180. SECRETARY OF THE U.S. DEPARTMENT OF THE TREASURY, A REPORT TO THE CONGRESS IN ACCORDANCE WITH SECTION 359 OF THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT OF 2001, at 6 (Nov. 2002) [hereinafter REPORT TO THE CONGRESS IN ACCORDANCE WITH SECTION 359].

181. *Id.* at 5.

182. *See* Pathak, *supra* note 174, at 2016.

183. REPORT TO THE CONGRESS IN ACCORDANCE WITH SECTION 359, *supra* note 180, at 5.

formal value transfer systems counterparts in the regulatory scheme, the transfer of illegal proceeds going to terrorists would still be difficult to detect.[184] The information that is provided by the IVTS reporting must be added to the vast amount of information already provided by formal value transfer systems. However, at the very least, those providing the *hawala* services will be required to keep adequate records that can be used by law enforcement officials, provided they comply with the regulations.[185] With the ever increasing regulations on the formal value transfer systems, *hawalas* would become a natural alternative to terrorists seeking to move money without leaving a trail.[186] While enforcement of these provisions may be difficult, it should not be overlooked by law enforcement agencies seeking to implement a comprehensive anti-money laundering strategy.

b. Know Your Customer

Section 326 of the Patriot Act required the "Secretary of the Treasury [to] prescribe regulations setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution."[187] These require banks and other financial institutions to maintain accurate records concerning the ownership of accounts.[188] The Act also requires financial institutions to compare the names of new owners to lists of known terrorists.[189]

For individuals that are residents of the U.S., obtaining proof of identity may be fairly simple. Generally a driver's license or passport is sufficient to establish identity.[190] If the customer is not a U.S. resident, identification still

184. *See* Pathak, *supra* note 174, at 2057–58.

185. *See* Gouvin, *supra* note 6, at 979 (proposing that there will not be substantial compliance within the *hawala* community due to a history of secrecy, and difficulty of identifying hawalas).

186. Intuitively, it would seem a natural alternative if terrorist access to the conventional banking systems were curtailed. However, there is evidence that the 9-11 hijackers "did not extensively rely on hawala networks." Pathak, *supra* note 174, at 2057.

187. Patriot Act, Pub. L. No. 107-56, § 326(a), 115 Stat. 272, 317 (2001) (codified as amended in 31 U.S.C. § 5318). The minimum requirements must include reasonable procedures for

> (A) verifying the identity of any person seeking to open an account to the extent reasonable and practicable; (B) maintaining records of the information used to verify a person's identity, including name, address, and other identifying information; and (C) consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

Id.

188. *Id.*

189. Michael F. McEneney, David E. Teitelbaum & Karl F. Kaufmann, *Customer Identification Requirements Under the USA Patriot Act*, 59 BUS. LAW. 1287, 1295 (2004).

190. *Id.* at 1292.

needs to be confirmed.[191] However, regulators have not been clear on exactly what types of foreign-issued identification will be sufficient.[192] "Know your customer" (KYC) provisions were not invented by the Patriot Act. They were first proposed in 1998, but banks and other depositary institutions fought strongly against them and won.[193] The banks expressed concern over the ever-increasing quantity of information that they were being required to present to the government, and over the eroding privacy of their customers.[194] However, concern for terrorism after 9-11 again won out when similar provisions were enacted by the Patriot Act.[195]

c. Anti-Money Laundering Program Provisions

Section 352 of the Patriot Act requires financial institutions included in the Act to establish programs to counter money laundering schemes.[196] This section of the Act requires "(A) the development of internal policies, procedures and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs."[197] Many banks and other financial institutions already had these programs in place, as they were established in the Annunzio–Wylie Anti-Money Laundering Act of 1992. The Patriot Act did not substantially alter the structure or requirements of these programs.

d. Information Sharing

Section 314 of the Patriot Act requires the Secretary of the Treasury to adopt regulations that will encourage cooperation between financial institutions, regulatory authorities, and law enforcement agencies.[198] This section also required banks to appoint a person to receive information

191. *Id.* at 1290.

192. *Id.* at 1290–91. Information sufficient to identify non-U.S. persons include a passport number, a taxpayer identification number, or an alien identification card number. 31 C.F.R. § 103.121 (b)(2)(i)(A)(*4*)(*ii*) (2003). However, the less specific portion allows the "number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard." *Id.*

193. Daniel Mulligan, Comment, *Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime*, 22 FORDHAM INT'L L.J. 2324, 2363–65 (1999). The KYC provisions in the Patriot Act are not quite as extensive as those originally proposed, as they are not designed to address ongoing review or monitoring of accounts. Pasley, *supra* note 100, at 209.

194. *See* McEneney et al., *supra* note 189, at 1295.

195. Zagaris, *supra* note 71, at 127–28.

196. Patriot Act, Pub. L. No. 107-56, § 352, 115 Stat. 272, 322 (2001) (codified as amended at 31 U.S.C. § 5318 (Supp. I 2003)).

197. *Id.*

198. *Id.* § 314(a)(1), 115 Stat. at 307.

regarding the subjects of the investigations and to monitor their accounts.[199] The section also provided for information-sharing between banks, and it relieved them of any liability for sharing the information or for failing to notify the subject of the information in the communication.[200] The Financial Crimes Enforcement Network has been charged with coordinating the requests between law enforcement agencies and the financial institutions.[201] The regulations issued by the Secretary do not give FinCEN the power to arbitrarily request information from financial institutions. When a request is made to a financial institution, FinCEN must certify, at a minimum, that the individual about which the law enforcement agency seeks information "is reasonably suspected based on credible evidence of engaging in[] terrorist activity or money laundering."[202] FinCEN must also provide "enough specific identifiers . . . that would permit a financial institution to differentiate between common or similar names."[203] It should be emphasized that while many parts of the Patriot Act may be over-inclusive, this section provides access to financial records in cases where terrorism is suspected.

There is some concern that this provision invades the privacy interests of the customers of the financial institutions.[204] However, given the Supreme Court's long established stance that the customer has no reasonable expectation of privacy in records maintained by the bank vis-à-vis the government, it would be difficult to challenge the requirements.[205]

5. International Action

The attacks on 9-11 also gave rise to increased international scrutiny of money laundering, specifically with respect to the financing of terrorist organizations. While the U.S. has always been a leader in the global community with respect to anti-money laundering legislation,[206] prior to 9-11, there were fundamental differences between the interests of the liberally governed European Union, and the more conservatively governed U.S.[207] The EU, and specifically the Organization for Economic Cooperation and Development (OECD) had already been pursuing bank secrecy and tax havens

199. *Id.* § 314(a)(3)(A), 115 Stat. at 307.

200. *Id.* § 314(b), 115 Stat. at 308.

201. 31 C.F.R. § 103.100(b) (2005).

202. *Id.* § 103.100(b)(1).

203. *Id.*

204. *See* Gouvin, *supra* note 6, at 983.

205. *See* discussion *supra* Part II.B.1.

206. This is partly because "the U.S. dollar has become the preferred currency of the [drug] industry and is inextricably intertwined with money laundering activities." Morgan, *supra* note 79, at 24.

207. *See* Lacey & George, *supra* note 16, at 331–32.

around the world.[208] However, their intent wasn't so much to curb terrorism or other underlying crimes as it was to increase tax revenue.[209] This conflicted with conservative groups in the U.S. interested in promoting international tax competition and attracting foreign investment,[210] not to mention with the interests of the Caribbean nations themselves. In May of 2001, then-Treasury Secretary Paul O'Neill issued a press release indicating that the U.S. would no longer support the OECD working-group targeting "harmful tax practices."[211] Although O'Neill stressed the need for information exchange, he indicated that the U.S. would not support it at the cost of eliminating international tax competition.[212] However, after 9-11 there was an interest in promoting international financial transparency that trumped the desire to promote tax competition.[213] The U.S. has entered into a number of Mutual Legal Assistance Treaties (MLAT) with foreign nations that provide for the exchange of information relating to criminal matters.[214] In the case of offshore tax havens such as the Cayman Islands, the treaties require that the offense be a crime in both jurisdictions, and hence do not allow the exchange of information for purely tax purposes.[215] This agreement allows the U.S. to request specified information regarding Cayman bank accounts from the Cayman authorities.[216] However, the information may be cumbersome to obtain.[217] New York County District Attorney Robert Morgenthau indicated his hope that the Patriot Act will allow quicker retrieval of foreign records.[218]

208. *See id.* at 330.

209. John Burton & Andrew Parker, *Is the Global Crackdown on Tax Evasion 'Slowing to the Speed of the Last Ship in the Convoy'?*, FIN. TIMES, Dec. 1, 2003, at 17.

210. *See* Lacey & George, *supra* note 16, at 331. The financial services industry accounts for 30 percent of the Cayman Islands' gross domestic product, and many predict that imposing strict money laundering regulations on the system might result in flight of capital from both the EU and the U.S. Burton & Parker, *supra* note 209, at 17.

211. Press Release, U.S. Dep't of the Treasury, Treasury Secretary O'Neill Statement on OECD Tax Havens (May 10, 2001), *available at* http://www.ustreas.gov/press/releases/po366.htm.

212. *Id.* Increased international financial reporting has largely been equated with the elimination of international tax competition, because the reporting requirements would allow governments to tax their citizens on foreign investment, thus eliminating the benefit of investing in tax havens.

213. Lacey & George, *supra* note 16, at 332.

214. Richard A. Westin, *Expatriation and Return: An Examination of Tax-Driven Expatriation by United States Citizens, and Reform Proposals*, 20 VA. TAX REV. 75, 127–28 (2000).

215. *Id.* at 127.

216. *Id.*

217. *Bridging the Tax Gap: Hearing Before the S. Comm. on Finance*, 108th Cong. 300 (2004) (statement of Robert M. Morgenthau, District Attorney of New York County).

218. *See id.* (indicating that the Patriot Act's requirement for "foreign banks with correspondent accounts in the U.S. to appoint an agent for service of process in this country, will

The system in place between the Cayman Islands and the U.S. can be seen as the opposite of the U.S.'s domestic reporting system. In the U.S., every large or otherwise suspicious activity is reported, resulting in millions of reports, many of which are completely legitimate. In the case of the Cayman Islands, the U.S. will not receive any information unless there is an objective reason that can be presented to the Cayman authorities.

The leading international body with respect to anti-money laundering laws is the Financial Action Task Force on Money Laundering (FATF).[219] The FATF was formed in 1989 at the G-7 Summit in order to address issues of international money laundering activity.[220] The FATF created a list of forty recommendations for countries wishing to prevent international money laundering.[221] These forty recommendations have been updated since 1990, when they were first established.[222] In October of 2001, the mission of the FATF was extended to include all types of international activities used to finance terrorism.[223] The FATF then created eight new recommendations specifically aimed at curbing terrorist financing.[224] These recommendations largely mirror legislation already enacted in the U.S. and discussed in Part II.B. of this Comment.[225] Two of the recommendations are specifically aimed at international cooperation.[226] The first recommends that all countries "ratify and . . . implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism."[227] The fifth recommends that countries establish by treaty information-sharing agreements with other countries.[228]

help to circumvent some of the current complexities and obstacles in the MLAT process, as it applies to foreign banks").

219. The FATF is made up of twenty-six member nations, all of whom have enacted some form of anti-money laundering legislation. Daley, *supra* note 40, at 187. The FATF "[r]ecommendations [were] the first to stress, in an international forum, the need for financial institutions to use their expertise to detect suspicious transactions and to notify the appropriate authorities." *Id.*

220. Barbot, *supra* note 75, at 173–74.

221. Sean D. Murphy, *Multilateral Listing of States as Money-Laundering Havens*, 94 AM. J. INT'L L. 695, 696 (2000).

222. *Id.* at 696 n.5.

223. Andrew Ayers, *The Financial Action Task Force: The War on Terrorism Will Not be Fought on the Battlefield*, N.Y.L. SCH. J. HUM. RTS. 449, 451 (2002).

224. Financial Action Task Force on Money Laundering, *Special Recommendations on Terrorist Financing* (Oct. 31, 2001), *available at* http://www.fatf-gafi.org/dataoecd/55/16/34266142.pdf.

225. *See id.*

226. *Id.*

227. *Id.* at ¶ I.

228. *Id.* at ¶ V.

The UN International Convention for the Suppression of the Financing of Terrorism was adopted on December 9, 1999.[229] The UN first addressed the issue of international money laundering in 1988 with the Vienna Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.[230] The International Convention for the Suppression of the Financing of Terrorism

> prohibits direct involvement or complicity in the international and unlawful provision or collection of funds, attempted or actual, with the intent or knowledge that any part of the funds may be used to carry out any of the offenses described in the Convention, such as those acts intended to cause death or serious bodily injury to any person not actively involved in armed conflict in order to intimidate a population, and any act intended to compel a government or an international organization to take action or abstain from taking action.[231]

In addition to prohibiting the act of money laundering, the Convention also requires signatories to take domestic action "for the detection, freezing, seizure, and forfeiture of any funds used or allocated for the purposes of committing the listed offenses."[232] These requirements involve KYC regulations and suspicious transaction reporting similar to those already in use in the U.S.[233] On September 12, 2001, in the wake of the attacks of 9-11, the UN Security Counsel adopted Resolution 1368 condemning the terrorist attacks and calling on member nations to adopt previous conventions regarding terrorism.[234]

III. THE BENEFITS OF CURRENT ANTI-MONEY LAUNDERING LEGISLATION

The BSA as amended by the Patriot Act provides valuable tools to law enforcement agencies not only in preventing the financing of terrorism, but also in other areas of the law. The tools included in the Patriot Act complement existing legislation and give law enforcement agencies the ability to more effectively trace the proceeds of money that is provided to terrorists both at home and abroad. Although it has been argued that the increased regulations on U.S. financial institutions will leave them at a competitive disadvantage with other less regulated countries, the financial institutions may

229. Gilbert Guillaume, *Terrorism and International Law*, 53 INT'L & COMP. L.Q. 537, 539 n.6 (2004).

230. Zagaris, *supra* note 71, at 137.

231. *Id.* at 138.

232. *Id.*

233. *Id.*

234. *Id.* at 139–40.

actually see some long-term benefit.[235] Further, the Patriot Act does not create any significant new privacy issues.

A. Benefits to Law Enforcement

The amendments to the BSA in the Patriot Act have already proven beneficial to law enforcement officials. FinCEN has established a direct case support program that functions as a clearing house for information collected pursuant to the Patriot Act.[236] FinCEN was established with the purpose of assisting all federal agencies with obtaining information relating to terrorist financing and money laundering.[237] Section 314(a) allows law enforcement agencies to request information regarding suspects, businesses, and accounts.[238] The requested information is then either provided using the information that FinCEN has already collected, or passed on to more than 20,000 financial institutions in an attempt to obtain the information.[239] FinCEN then coordinates the retrieval of the information from the financial institutions and directs the law enforcement agency to the source of the information.[240] According to FinCEN, its direct case support program "provides an average of 5,000 analytical case reports each year involving over 25,000 individual subjects annually to federal, state, local, and international agencies."[241] During the period from February 2003 to June 2004, FinCEN reports that the inquiries resulted in 1,236 new accounts located, 73 new transactions identified, 601 grand jury subpoenas served, eleven search warrants executed, nine individuals indicted, and two individuals arrested.[242] The fact that this may seem like a small number of individuals indicted and arrested considering the scope of the regulatory scheme should not necessarily be considered a failure. The success of the program would not necessarily

235. *See, e.g.*, George A. Lyden, *The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001: Congress Wears a Blindfold While Giving Money Laundering Legislation a Facelift*, 8 FORDHAM J. CORP. & FIN. L. 201, 229–37 (2003).

236. Financial Crimes Enforcement Net, U.S. Dep't of the Treasury, Law Enforcement / Direct Case Support, http://www.fincen.gov/le_directcasesupp.html (last visited Mar. 24, 2006); *see also* Patriot Act, Pub. L. No. 107-56, § 314(a), 115 Stat. 272, 307 (2001).

237. Financial Crimes Enforcement Net, U.S. Dep't of the Treasury, Law Enforcement / Direct Case Support, http://www.fincen.gov/le_directcasesupp.html (last visited Mar. 24, 2006).

238. *Terrorist Financing and Money Laundering Investigations: Who Investigates and How Effective Are They?: Hearing Before the Subcomm. on Criminal Justice, Drug Policy, and Human Resources of the H. Comm. on Government Reform*, 108th Cong. 92 (2004) (statement of Robert W. Werner, Chief of Staff, FinCEN, Dep't of the Treasury).

239. Financial Crimes Enforcement Net, U.S. Dep't of the Treasury, Law Enforcement / Direct Case Support, http://www.fincen.gov/le_directcasesupp.html (last visited Mar. 24, 2006).

240. *Id.*

241. *Id.*

242. BANK SECRECY ACT ADVISORY GROUP, 7 SAR ACTIVITY REV. 29–30 (2004), *available at* http://www.ots.treas.gov/docs/4/480025.pdf.

hinge on the number of indictments, but rather the ability to provide valuable information to other law enforcement agencies.

The direct case support program operated by FinCEN provides information to programs such as the Terrorist Financing Operations Section (TFOS) of the FBI's Counterterrorism Divison.[243] This section was formed in response the perceived shortcomings in the FBI's ability to analyze terrorist financing efforts shortly after 9-11.[244] Using the information collected pursuant to the Patriot Act, TFOS utilizes the data for a variety of purposes including: (1) "conducting full financial analysis of terrorist suspects and their financial support structures in the US and abroad"; (2) "developing predictive models and conducting data analysis to facilitate the identification of previously unknown or 'sleeper' terrorist suspects"; and (3) "providing the financial component to classified counterterrorism investigations in support of the FBI's counterterrorism responsibilities."[245]

While some have criticized the ability of the Patriot Act to ferret out individual acts of terrorism, the purpose of the Act is to complement other areas of law enforcement, rather than to replace them. The 9-11 Commission emphasized this in its report, finding that "[c]ounterterrorism investigations often overlap or are cued by other criminal investigations, such as money laundering."[246] The Act is being used in conjunction with traditional intelligence and law enforcement methods to attack the "financial substructure of terrorist groups."[247] Juan Carlos Zarate, the assistant secretary of the Treasury for terrorist financing, has emphasized that "[f]inancial records and audits provide blueprints to the architecture of terrorist organizations."[248] This information helps law enforcement agencies determine the sources of terrorist funding, and diminishes the terrorists' ability to recruit members, carry out attacks, and purchase dangerous weapons.[249]

B. The Competitive Position of U.S. Financial Institutions

Financial institutions have been subject to reporting requirements for over thirty years and yet have maintained their competitive position in the world market. When the legislation was first introduced, a senior counsel for the

243. *The 9-11 Commission*, *supra* note 7, at 5 (statement of John E. Lewis).

244. *Id.* at 3.

245. *Id.* at 4; *see also* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2004) (suggesting that the public should be active, rather than resistive, in developing computer models that determine suspicious patterns, and that this would in the long run lead to more liberty, rather than less).

246. THE 9-11 COMMISSION REPORT, *supra* note 1, at 424.

247. Juan Carlos Zarate, *Bankrupting Terrorists*, EJOURNAL USA: ECON. PERSPECTIVES, Sept. 2004, at 3, 4, *available at* http://usinfo.state.gov/journals/ites/0904/ijee/ijee0904.pdf.

248. *Id.* at 3.

249. *Id.*

American Bankers Associations stated that "[t]he practical effect will be fairly minimal," and the legislation "simply puts into statute what happens daily in a financial institution."[250] The additional reporting requirements of the Patriot Act are unlikely to substantially alter their competitive position. Moreover, the reporting process is consistently becoming more efficient. FinCen has recently put into operation the Patriot Act Communication System (PACS), which will allow many financial institutions to send CTRs and SARs electronically, and in batches.[251] Electronic submission of required reports will not only reduce costs to the financial institutions in the form of time and materials, but will allow the reports to be processed more efficiently.[252] However, the number of reports that are filed needs to be, and can be under the current regulatory scheme, reduced significantly if the reports are to be used efficiently.[253] Congress has called for regulations that would decrease the number of reports filed each year multiple times.[254] Reducing the number of reports would have a number of effects. One would be to reduce the burden on banks by allowing them to more selectively determine which transactions to report. Another would be the increased ability of federal agencies to more thoroughly analyze the remaining reports.[255] The budget of FinCEN is currently insufficient to provide adequate resources to analyze the number of reports currently being submitted.[256] This does not encourage timely and consistent filing by financial

250. Couture, *supra* note 76, at 21.

251. Press Release, Financial Crimes Enforcement Network, U.S. Dep't of the Treasury, FinCEN Expands E-Filing System: Financial Institutions Begin Filing BSA Reports over Secure Internet (Oct. 1, 2002), *available at* http://www.fincen.gov/newsreleasepacs10012002.pdf. The Director of FinCEN has indicated that he would like to reduce the number of SARs being filed, focusing more on quality than on quantity. William J. Fox, Director, Financial Crimes Enforcement Network, U.S. Dep't of the Treasury, Remarks at the American Bankers Assn. / American Bar Assn. Money Laundering Enforcement Seminar (Oct. 25, 2004), *available at* http://www.fincen.gov/fox102504.pdf. [hereinafter Remarks of William J. Fox].

252. Gouvin, *supra* note 6, at 969.

253. *See Oversight of the Department of the Treasury: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Services*, 108th Cong. 74 (2004) (statement of Nancy Jardini, Chief, Criminal Investigation, Internal Revenue Service) (reporting that nearly 14 million currency forms were filed in 2003).

254. *See* Gouvin, *supra* note 6, at 968 (explaining that Congress attempted to reduce the number of CTRs being filed through the Money Laundering Suppression Act of 1994); *see also* Patriot Act, Pub. L. No. 107-56, § 366, 115 Stat. 272, 298 (2001) (calling for more efficient use of the CTR reporting system).

255. The Director of FinCEN has indicated that he would like to reduce the number of SARs being filed, focusing more on quality than on quantity. Remarks of William J. Fox, *supra* note 251; *see also* Patriot Act, Pub. L. No. 107-56, § 366(a)(2)–(3), 115 Stat. 272, 335 (2001) (finding that a large number of CTRs that could otherwise be exempted from the process are being filed, and that the over-reporting is interfering with effective law enforcement); H.R. REP. NO. 101-446, at 24 (1990) (emphasizing the importance of the reporting system, but calling on banks to properly exempt certain transactions in order to alleviate the over reporting of CTRs).

256. Roberts, *supra* note 76, at 596–97.

institutions. FinCEN has also expressed concern over the practice of "defensive" reporting with regard to SARs.[257] Due to the increased scrutiny of anti-money laundering compliance after the enactment of the Patriot Act, many financial institutions have been over-reporting suspicious activity for fear of being penalized.[258] Another factor that contributes to over-reporting suspicious activity may be the "safe harbor" provisions that protect banks from liability for unjustifiably filing an SAR.[259]

Both the FBI and FinCEN have been implementing data analysis of current and past reports that will allow them to develop more clear guidelines for use in determining when certain reports should be filed.[260] FinCEN's efforts to automate the reporting system should allow them to analyze the data faster, and provide important feedback to the institutions.[261] Furthermore, section 314(d)(1) of the Patriot Act specifically requires the Secretary of the Treasury to "publish a report containing a detailed analysis identifying patterns of suspicious activity and other investigative insights derived from suspicious activity reports and investigations conducted by Federal, State, and local law enforcement agencies to the extent appropriate," and to provide this information to financial institutions.[262]

The financial institutions regulated by anti-money laundering legislation are in a unique position to administer the programs, as much of the information that is required, particularly by the "know your customer" (KYC) provisions, would be obtained through the regular practices of the bank.[263] As far back as 1997, banks have been encouraged to develop KYC programs on their own initiative, as the information is often needed to properly file reports required by other provisions of the BSA such as SARs and CTRs.[264] Further, many of these financial institutions are controlled by shareholders, or at the least by an owner interested in profits. Therefore, the owners or shareholders have a

257. Remarks of William J. Fox, *supra* note 251.

258. *Id.* Financial institutions may also over-report out of fear that sanctions may injure their reputation. *Id.*

259. Patriot Act, Pub. L. No. 107-56, § 351, 115 Stat. 272, 320–21 (2001) (codified as amended at 31 U.S.C. § 5318(g)(3) (Supp. I 2003)).

260. *Oversight of the Department of the Treasury: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Services*, 108th Cong. 53 (2004) (written testimony of Samuel W. Bodman, Deputy Secretary, U.S. Dep't of the Treasury). A small number of SARs are currently being filed electronically. *Id.* While electronic filling sometimes burdens institutions that do not file reports frequently, on the whole it has been found to be faster and more accurate than manual filing. *Id.*

261. *Id.*

262. Patriot Act, § 314(d)(1), 115 Stat. at 308.

263. *See* McEneney, et al., *supra* note 189, at 1290 (describing the findings of the regulating agencies that banks will generally obtain information regarding identification through regular business practices, or in order to comply with other provisions of the BSA).

264. Morgan, *supra* note 79, at 47.

vested interest in ensuring that the programs are administered in the most efficient manner possible.

The Patriot Act has a substantial effect on foreign financial institutions that wish to do business in the U.S.[265] This effect will require many financial institutions, most of which cannot afford to surrender their access to the largest financial market in the world, to maintain policies with regard to record keeping similar to U.S. financial institutions.[266] This will therefore lessen any competitive disadvantage that would arise from the U.S. regulatory scheme. Also, many of the provisions enacted in the Patriot Act are being advocated by the U.S. and international organizations in other areas of the world, including other major banking systems.[267] Due to the increasing ease of transferring money between different financial institutions in the different countries, it is clear that money laundering cannot be addressed by concentrating on only domestic enforcement. International organizations such as the FATF have been attempting to implement more stringent reporting requirements across the globe.[268] In fact, many components of the Patriot Act mirror the anti-money laundering provisions that are included in the FATF's Nine Special Recommendations on Terrorist Financing ("Nine Special Recommendations"), and the U.N. Security Counsel's Regulation 1373.[269] For instance, one of the Nine Special Recommendations is that "[i]f financial institutions[,] or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities."[270] This was implemented in the U.S. through the use of SARs and by requiring other financial institutions besides banks to implement reporting procedures. Another of the Nine Special Recommendations that was codified in U.S. law is

265. *See generally* Morris, *supra* note 155 (describing the effects of the Patriot Act).

266. *Id.* at 387.

267. Zarate, *supra* note 247, at 5; Karlin Lillington, *Tech Advances Make It Harder to Clean Dirty Money*, IR. TIMES, Mar. 5, 2004 (explaining that Ireland and the UK are taking similar efforts to eradicate money laundering).

268. *See* Matthew R. Hall, *An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering, and the Suspicious Activity Report*, 84 KY. L.J. 643, 675 (1996) (discussing reporting requirements in foreign countries including the UK, Australia, and Hong Kong); *see also* Ricardo A. Pellerano & Eduardo Jorge, *Money Laundering Rules in the Domincan Republic*, 114 BANKING L.J. 136, 136 (1997) (discussing how authorities in the Dominican Republic have relied on financial institutions in a manner similar to the United States); *Anti-Money Laundering Laws to Be Tightened*, SWISSINFO, Jan. 12, 2005, *available at* http://www.swissinfo.org/sen/Swissinfo.html?siteSect=105&sid=5462518 (discussing an announcement by the Swiss Finance Ministry to attempt to comply with all Recommendations of FATF).

269. Zarate, *supra* note 247, at 4.

270. Financial Action Task Force on Money Laundering, Nine Special Recommendations on Terrorist Financing IV (Oct. 22, 2004), *available at* http://www1.oecd.org/fatf/SRecsTF_en.htm.

Special Recommendation VI, which recommends the licensing and registration of informal value transfer systems.[271] Most of the other Nine Special Recommendations can also be found codified in U.S. law.[272] As off-shore banking centers come under increased scrutiny for enabling criminals and terrorists alike, it is likely that the major financial powers in the world will demand more transparency.[273] The U.S. could benefit from establishing a comprehensive anti-money laundering program now, before they are forced to in order to participate in the global financial system.

C. Privacy Concerns

Although there are privacy concerns, there is little evidence that in the thirty years since the BSA has been enacted it has been significantly abused. Many commentators arguing that the reporting requirements violate the privacy of customers have referred to the violations in the abstract, rather than providing specific examples of abuses. Critics of the requirements rarely can point to specific instances of privacy violations. It can also be argued that the minimal invasion of privacy incurred when simple financial information is disclosed to the government is justified by the dangers that money laundering and terrorism pose to the global financial structure.[274] Although there is a risk of bogging down the financial industry with over-regulation, there is a greater risk involved with allowing the financial industry to be corrupted by criminal activity.

The KYC provisions of the Patriot Act have been particularly heavily criticized. However, as mentioned before, the KYC provisions merely codify a practice that generally is needed by banks to comply with SAR and CTR reporting.[275] The KYC provisions may even lead to an increase in privacy. If a bank is satisfied that it has correctly ascertained the identity of a customer, and has some information regarding the transactional history, then transactions that may have seemed suspicious if isolated will no longer be considered suspicious.[276] Congress has provided for certain situations where transactions that would otherwise be subject to reporting requirements are exempt because

271. *Id.* at VI.

272. A self assessment of U.S. compliance with the Recommendations is available online at http://www.treas.gov/offices/international-affairs/standards/code9-terror_financing.pdf.

273. *See* Patriot Act, Pub. L. No. 107-56, § 302(a)(4), 115 Stat. 272, 296 (2001) (finding that "'offshore' banking and related facilities designed to provide anonymity, coupled with weak financial supervisory and enforcement regimes, provide essential tools to disguise ownership and movement of criminal funds").

274. Sarah N. Welling, *Smurfs, Money Laundering, and the Federal Criminal Law: The Crime of Structuring Transactions*, 41 FLA. L. REV. 287, 310 (1989).

275. *See supra* Part II.B.4.

276. Peter E. Meltzer, *Keeping Drug Money from Reaching the Wash Cycle: A Guide to the Bank Secrecy Act*, 108 BANKING L.J. 230, 239 (1991).

of the minimal risk they pose.[277] Therefore, it seems that what is actually under attack are the reporting requirements themselves, which have been in effect for a considerable length of time. The validity of these reporting requirements has been upheld since the Court decided in favor of the process in *California Bankers Ass'n*.[278] Further, in *U.S. v. Miller*,[279] the Supreme Court held that bank customers did not have the right to challenge subpoenas issued by the government to obtain bank records.[280] Therefore, even if government investigators were required to obtain subpoenas for every request of information, the banks, rather than the customers, would be responsible for challenging the subpoenas.

Further, the KYC provision that requires financial institutions to compare the names of customers to lists of suspected terrorists may be one of the most effective means of detecting terrorist financing.[281] According to FinCEN, since the implementation of the policy, "the system has been used to send the names of 1,547 persons suspected of terrorism financing or money laundering to more than 26,000 financial institutions and has produced 10,560 matches that were passed on to law enforcement."[282]

IV. CONCLUSION

While some critics have claimed that the anti-money laundering laws as written will not protect the U.S. from terrorism in the future, they may be viewing the issue too myopically. Although many of the changes may not be able to ferret out individual acts of terrorism, they will substantially limit access to U.S. financial systems to terrorists, and make it more difficult to move money. It will also identify the sources of terrorist funding, allowing law enforcement to attack terrorism at its base. Implementing such a comprehensive money laundering strategy will no doubt take time to work out the problems.[283]

277. *Id.* at 235–36; *see also* Pasley, *supra* note 100, at 200 ("To the extent the conduct reflects the normal, appropriate activity of a business, an extensive process exists within the BSA for exempting such businesses.").

278. California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974).

279. 425 U.S. 435 (1976).

280. *Id.* at 444 (explaining that subpoena did not violate Fourth Amendment because customer had no reasonable expectation of privacy in records that were turned over to a third party, and subsequently provided to the government). If the customer has no reasonable expectation of privacy in the records that he makes available to his bank, then it is unlikely that a court would find that the SAR violates the Fourth Amendment, even in the absence of a subpoena.

281. Zarate, *supra* note 247, at 4.

282. John J. Byrne, *Banks and the USA PATRIOT Act*, EJOURNAL USA: ECON. PERSPECTIVES, Sept. 2004, at 18, 21, http://usinfo.state.gov/journals/ites/0904/ijee/ijee0904.pdf.

283. Zagaris, *supra* note 71, at 156.

Title III of the Patriot Act is not a perfect instrument for combating the financing of terrorism. However, given the scale of international money laundering, and the extent of global terrorist networks, it would be difficult to establish any piece of legislation that could put a significant dent in present levels of criminal activity. The American people are right to be concerned about privacy and their civil liberties. With this in mind, it should be observed that at least with respect to Title III of the Patriot Act, the general balance between privacy and security has remained largely unchanged. While the Patriot Act has expanded the number of institutions that are subject to reporting requirements, and codified minimum due diligence procedures, it has not significantly invaded our private lives beyond what has been law for over thirty years. The Patriot Act addresses important loopholes in the anti-money laundering scheme that have been exploited to the detriment of the financial system. It also provides a much needed focus on the international nature of money laundering. The balance between privacy and security is an important discussion, but the issue should be the overall anti-money laundering scheme, rather than simply the Patriot Act. The Patriot Act provides valuable tools to law enforcement, without significantly intruding on civil liberties, and should therefore be extended by Congress past the scheduled sunset date.

PAUL FAGYAL*

* Saint Louis University School of Law, J.D. Candidate 2006. I would like to thank my wife for her love and support. I would also like to thank Professor Nan Kaufman for her assistance.